

Test de Intrusión: Reconocimiento y Enumeración

1. Footprinting: Se obtiene una "instantánea" de los elementos observables en la red local (IP activas, protocolos usados, topología, si hay IDS/IPS...)
2. Fingerprinting: Una vez identificadas las máquinas en la red, se escanean para obtener información de estas (Sistema operativo y su versión, servicios activos y sus versiones, Info del IDS o firewall desplegado)

Reconocimiento

- Activo: Interacción directa con el objetivo, se tiene interacción directa con la organización victima. Hay un alto riesgo de detección, se usan barridos de ping o conexiones de puertos de alguna aplicación.
- Pasivo: No se tiene interacción con el objetivo. Se obtiene mediante google, IP o puertos abiertos. Se usa Sniffing.

[L2] Capa de enlace

Se suele realizar el descubrimiento de esta capa mediante el uso del protocolo ARP para descubrir servicios sin ser detectado, para ello se usan las siguientes herramientas:

- ARPing
 - Envía una trama ARP en la capa de enlace como si fuera un ping en la capa de red
 - Útil en máquinas con el ping deshabilitado
 - Evita detección por firewalls básicos

```
arping 192.168.56.6 -c 1
```

- Netdiscover: similar a a ARPing

```
#Para una interfaz
```

```
netdiscover -i eth0
```

```
#Ficheros de entrada
```

```
netdiscover -l lista_ips.txt
```

```
#Ragos de IP
```

```
netdiscover -r 192.168.56.0/24
```

```
#Modo pasivo (Muy lento)
```

```
netdiscover -p
```

- NMAP: Permite evitar el envío de ping
 - Sondeo de lista (-sL)
 - Deshabilitación de ping (-Pn)
 - Enviando combinaciones arbitrarias de sondas

- Metasploit
 - [Escaneo y Explotación de vulnerabilidades con Metasploit](#)
 - [\[Intrusión Extra\] Metasploit para dummies](#)

Las herramientas utilizadas en esta capa están limitadas debido a que las solicitudes ARP no atraviesan los routers y solo detectan sistemas de la misma subred

[L3] Capa de red

El descubrimiento en capa 3 se basa en ICMP.

- fping: versión de ping optimizada para escaneos simultáneos. En lugar de enviar paquetes a un solo objetivo hasta que pase cierto período de tiempo, envía un paquete ping y pasa al siguiente objetivo.
 - El flag “-a” muestra los sistemas activos
 - El flag “-g” genera una lista desde la máscara de red IP proporcionada o una IP de inicio y otra de fin.
 - Si se define una red con máscara de red, las direcciones de red y broadcast serán excluidas.
- hping3: Además de paquetes ICMP, también puede enviar TCP, UDP y RAW-IP.

```
#Permite trazar rutas de conexión y evadir reglas de firewalls
hping3 udc.gal -t 1 --traceroute
```

```
#Permite realizar ataques DDOS y DOS:
hping3 --rand-source 192.168.56.6
hping3 --rand-source --flood 192.168.56.4
```

- NMAP: se puede realizar escaneo de red mediante flag “-sn”. Para evitar el uso de ARP se inserta el flag “-disable-arp-ping”

[L4] Capa de transporte

Basado en TCP/UDP. Hay que distinguir entre descubrimiento (Detectar máquinas) y enumeración (escaneo de puertos). En este tipo de descubrimiento se suelen utilizar los puertos conocidos para saber si una máquina está apagada.

- hping3

```
#Se escanean puertos conocidos con el flag SYN de TCP
hping3 --udp 192.168.56.4 -p 53
```

```
#Se escanean puertos conocidos por UDP (Si devuelve flag SA, el puerto está abierto, si devuelve RA, entonces está filtrado o cerrado.)
hping3 -S udc.gal -p 80
```

```
#Se puede ver cuanto tiempo lleva la máquina arrancada
```

```
hping3 -p 443 -S --tcp-timestamp udc.gal
```

- NMAP

```
#Escaneo de puertos conocidos usando flag SYN de TCP
```

```
nmap 192.168.56.4 -PS80 -sn
```

```
#Escaneo de puertos conocidos usando flag ACK de TCP
```

```
nmap 192.168.56.4 -PA80 -sn
```

```
#Escaneo de puertos conocidos por UDP
```

```
nmap udc.gal -PU53 -sn
```

From:

<https://www.knoppia.net/> - **Knoppia**

Permanent link:

https://www.knoppia.net/doku.php?id=master_cs:int:tm2v2&rev=177910022

Last update: **2026/05/18 10:27**

